RE Abstract of my presentation in SWITS 2010.txt

Fu Zhang, Chalmers TH:

A Denial-of-Service (DoS) attack is an attempt from the attacker to prevent the legitimate users of a service from using that service.
The attacker may aim at subverting the legitimate communications of some specific applications or exhausting the bandwidth of the target hosts.
Knowing that the static open ports for applications may become the targets of DoS attacks, we build on the a port-hopping method suggested earlier and extend it for multiparty applications to
deal with such threat with the presence of time uncertainty.
Distributed Denial of Service (DDoS) attacks are more powerful and are more difficult to defend against, since the attacking sources are hard to be traced and the attacker can combine various attacking means. Furthermore, since DDoS attacks are often bandwidth-exhaustion attacks and since the attacking sources are distributed among the network, it is preferable to control the malicious traffic distributedly and as closely to the sources as possible.
In our work we also propose methods which can mitigate or prevent Distributed Denial of Service attacks with the above goal, namely to give secure and robust ways that can sort out malicious traffic accurately, meanwhile keeping the network performance degradation as little as possible. Links to our research papers:

http://publications.lib.chalmers.se/cpl/record/index.xsql?pubid=121109